EXHIBIT 1

Recent Releases

6.6.25

Product Update
2020-06-03

Fixes

- We fixed an issue that occasionally prevented the Security Console from marking completed scans with the "Completed" status if the console underwent a restart while the scans were in progress.
- We fixed an issue that could result in an invalid Google Chrome version being reported if the scanned asset had Citrix software installed.
- We fixed an issue where an incorrect default service name for PostgreSQL appearing in the `default-services.properties` file was causing authentication errors when using this name to assign the service to a custom port in a scan template.
- We updated several Microsoft vulnerability checks to use file versions instead of CBS-based registry entries in order to improve their accuracy.
- We updated our vulnerability checks for Microsoft Security Bulletin MS16-122 to improve accuracy on Server editions of Windows.

6.6.24

Product Update
2020-05-28

Fixes

- We reverted a previous change that we applied to our asset correlation process in product version 6.6.14. The strict unique ID enforcement requirement delivered in the previous fix was causing duplicate assets to appear in some Security Consoles.

6.6.23

Product Update
2020-05-27

New

- **New vulnerability content:** We added remote checks for CVE-2020-11651 and CVE-2020-11652, 2 vulnerabilities affecting SaltStack Salt Master servers. For more information on these vulnerabilities, see the SaltStack blog.
- **New vulnerability content:** We added a check that allows you to scan for obsolete versions of Arista EOS.
- **New AWS asset identification capability:** The Scan Engine will now collect AWS EC2 instance IDs if it can successfully authenticate to the target asset. Implementing this collection capability requires some configuration based on the asset type:
  - For Unix assets, your authentication user must have `sudo` or `root` access and the `curl` command must be available.
  - For Windows assets, you must configure the Windows Remote Management (WinRM) service on the target asset.

Improvements

- **Center for Internet Security (CIS) Policy content:** We updated our CIS Microsoft Windows 10 Enterprise Release 1809 benchmark to version 1.6.1.

Fixes

- Our Google Chrome fingerprinting process for Windows now relies on uninstaller keys to detect Chrome if registry keys are not available.
- Our CIS Microsoft Windows Server 2019 policy now supports rule customization that is similar to what is available in the 2016 edition policy.
- We fixed an issue with our CIS Oracle Database 12c benchmark (v2.1.0) where rule 4.5.2 was missing from some profiles.
- We fixed an issue with our CIS Red Hat Enterprise Linux 6 benchmark (v2.1.0) where rule 5.4.1.5 was missing from some profiles.
- We updated some Oracle Java vulnerability titles for better readability.

6.6.22

Product Update
2020-05-20

Improvements

- **Constraint validation service scheduling:** You can now configure the database constraint validation and remediation service to run on a schedule.

Fixes

- We optimized the Data Warehouse export process to improve performance when exporting large amounts of assets.
- Deleting multiple items from the notification center will no longer make the top and left menus invisible.
- We fixed CVE-2020-7353, a cross site scripting vulnerability affecting the Security Console. To exploit this vulnerability, an attacker would either have to execute a dynamic script in an attempt to assume control of a user's Security Console session, or modify HTML elements in real time in a way that would mislead the user into volunteering credential information. This issue affects all Security Console versions up to and including 6.6.20. If your Security Console currently falls on or within this affected version range, ensure that you update your Security Console to the latest version. Special thanks to Sandi Tehendi for reporting this issue.
- We fixed an issue that prevented users from checking scan results in policy detail pages if the web interface was accessed using a hostname as the URL instead of the Security Console's IP address.
- We fixed an issue where Security Console users that were configured to use SAML authentication could not run any console diagnostics.
- We fixed an issue that prevented our Adobe Acrobat and Reader DC 2015 vulnerability checks from generating correctly.
- We fixed an issue with our **unix-user-home-dir-mode** vulnerability check that caused the proof to display the returned directory permissions incorrectly.

6.6.21

Product Update
2020-05-13

New

- **New vulnerability content:** We added new checks for the following vulnerabilities affecting Cisco ASA that are part of the larger May 2020 Cisco Event Response Security Advisory Bundled Publication (ERP-73830):
  - CVE-2020-3187
  - CVE-2020-3125
  - CVE-2020-3259
  - CVE-2020-3254
  - CVE-2020-3196
  - CVE-2020-3298
  - CVE-2020-3191
  - CVE-2020-3195
- **Microsoft Patch Tuesday coverage:** This release includes updated scan coverage for May 2020.
- **New DISA policy content:** We added 2 new Defense Information Systems Agency (DISA) policies that provide coverage for Apache Server 2.4 UNIX Server and Site, respectively.

Improvements

- **Standalone constraint validation service:** The database constraint validation and remediation service that used to be tied exclusively to the backup creation process is now available as a standalone feature. Navigate to **Administration > Maintenance, Storage, and Troubleshooting > Maintenance > Validate Constraints** in your Security Console to run this service independently.
- **General interface improvements:** We implemented several interface changes to improve your Nexpose product experience:
  - The Security Console's top and left menu styles have been updated.
  - The notification center in the upper right corner of the interface has been reworked.
  - We fixed an issue with the left menu that caused the Rapid7 logo to block menu items on screens using lower resolutions.
- **Improved detail page performance:** Asset detail pages now load faster.
- **Center for Internet Security (CIS) Policy content:** We updated the following existing CIS benchmarks:
  - CIS Microsoft Windows Server 2008 R2 Benchmark v3.2.0
  - CIS Microsoft Windows 7 Workstation Benchmark v3.2.0
- **Improved SSH support:** The Scan Engine now supports SSH connections with larger Diffie-Hellman key exchange sizes for credentialed scanning.

Fixes

- We fixed an issue in the APIv3 documentation that caused some semantic and structural errors with OpenAPI Specification v2.0.
- We fixed an issue that caused some CIS database policies rules to evaluate incorrectly.
- We fixed an issue with our Oracle Java fingerprinting process where Java's installation location on UNIX targets was not properly recorded.

- We fixed an issue that allowed the product to run specific UNIX-based collection processes on Windows systems during a scan.

6.6.20

Product Update
2020-05-07

Fixes

- We fixed an issue where scan templates that specified an invalid regular expression in the regular expression file filter caused the Security Console to start up in maintenance mode after updating to product version 6.6.18.

6.6.19

Product Update
2020-05-06

New

- **New automated vulnerability content:** We now support recurring vulnerability coverage for Amazon Linux 2.

Improvements

- **Defense Information Systems Agency (DISA) Policy content:** We updated the following existing DISA benchmarks:
  - Red Hat Enterprise Linux 7 STIG Benchmark - Ver 2, Rel 7
  - Red Hat Enterprise Linux 6 STIG Benchmark - Ver 1, Rel 27
  - Mozilla Firefox for RHEL STIG Benchmark - Ver 1, Rel 6
  - Windows Defender Antivirus STIG Benchmark - Ver 1, Rel 6
  - Microsoft .NET Framework 4 STIG Benchmark - Ver 1, Rel 7
- **Updated obsolete version content:** We updated our **f5-big-ip-obsolete-version** check to include more unsupported versions.
- **Improved credential source labeling:** The "Administrative Credential" and "Service Credential" labels in scan logs and Source columns of node fingerprint tables have been renamed as "Configured Credential" and "Discovered Credential" respectively. These new labels will help you easily determine if the source credential that produced the fingerprint was configured by a user on the Security Console or discovered automatically during a scan.
- **Improved Apache Tomcat fingerprinting:** Our new fingerprinting technique can now identify Apache Tomcat on Windows assets using uninstaller registry keys.
- **Improved Linux vulnerability assessment capability:** The product will no longer report Linux kernel vulnerabilities that have been live-patched by KernelCare.

Fixes

- We fixed an issue with our **msft-cve-2020-0688-unsupported-version** vulnerability check to resolve potential false positives.
- We fixed several end-of-life checks for various Linux distributions that were missing the `Obsolete Software` category.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.